Testimony: Subcommittee on Financial Institutions and Consumer Credit
June 24, 2003
Testimony of Maureen V. Mitchell

Committee on Financial Services
2129 Rayburn House Office Building
Washington, D.C. 20515

Subcommittee on Financial Institutions and Consumer Credit
"Fighting Identity Theft ~ The Role of FCRA"

Statement of Maureen V. Mitchell: Ohio Identity Theft Victim

Mr. Chairman, Members of the Committee, my name is Maureen Mitchell and it is a privilege to have been invited to submit this testimony.

I am 47 years old, my husband Ray and I have been married for 26 years. We have a daughter in medical school and a son in college. I was born and raised in Woodside, New York. I was educated at Stuyvesant H.S. and Hunter College, CUNY. We have resided in Ohio since 1978. I am a Registered Nurse, and have been a licensed Realtor for 23 years.

My husband and I have always been financially prudent and fiscally responsible. We have always paid our bills in a timely manner, and we manage our finances prudently and responsibly. We have always exercised the normal consumer precautions to ensure our privileged financial information remains private. We have never lost our wallets, never been burglarized, we obtain the credit card receipts when we use our credit cards, we do not give our credit cards to waiters in restaurants, we do not bank on the Internet, we don't order merchandise via the Internet, and we shred our paper trash to prevent someone from "dumpster diving" and obtaining our personal information. We have never given our social security numbers out over the phone, and we had our social security numbers removed from our driver's licenses. We had also checked our credit reports in March of 1999 to ensure their accuracy.

In spite of all of the consumer precautions we have taken, we have become the unfortunate victims of Identity Theft. And, we were not only victimized once, we were victimized twice.

We first became aware of a fraud problem on September 12, 1999, when we received a phone call at home from a KeyBank service representative. Our KeyBank issued MasterCard account number was compromised and used by criminals to place fraudulent mail order purchases. We had never lost our credit cards, yet criminals somehow obtained our credit card account number and made fraudulent phone order purchases from an Illinois department store. The KeyBank service representative was calling because of an "unusual pattern of activity" on our credit card account. After much discussion, it was finally established with the service center representative that we

had not made or authorized the fraudulent charges. The service representative told me that KeyBank required us to report our credit cards as "lost or stolen". We objected to reporting our cards lost or stolen: my husband had his credit card in his wallet, and I had my credit card in my wallet. We were not given the option of closing the account at the request of the consumer due to fraudulent usage. Our credit card account was closed and we were to be issued new credit cards with a different account number. KeyBank never advised us to place Fraud Alerts on our credit reports, and said filing a police report was optional. I did file a police report with our local police department, and KeyBank launched an investigation. If KeyBank would have advised us to place Fraud Alerts on our credit reports, the following events may not have occurred.

On November 15, 1999 we received a phone call from JC Penney's credit department informing us that someone had used my husband's name and social security number to open an account at the JC Penney store at the Woodfield Mall in Schaumberg, Illinois. JC Penney became aware that the application was fraudulent when the bill was sent to the address given by the criminals on the fraudulent application. The bill was returned by the post office stamped saying "no such house number exists". The inability to deliver the bill was what prompted JC Penney to contact us. I informed the JC Penney representative of our KeyBank MasterCard account fraud, and was then advised by the JC Penney representative to contact the three major credit reporting agencies to place fraud alerts on our credit reports. I immediately called Trans Union, Experian and Equifax and placed the fraud alerts on our credit reports. Upon contacting Trans Union, Experian and Equifax, I was appalled to discover that we had been plunged into Identity Theft hell.

In speaking with Trans Union representative, I learned there had been 25 inquiries into our Trans Union credit report between September and November 1999. None of these inquiries were initiated by us legitimately seeking credit. I told the representative at Trans Union that there had not been 25 inquiries into our credit in the previous twenty years, and questioned whether that many inquiries in such a short period of time sent up "red flags' to Trans Union. The reply I received from the Trans Union representative was that it was not their job to monitor the number of inquiries, and it was suggested that I call all the merchants who made the inquiries. Trans Union provided me with the names and phone numbers of the merchants to contact. The list was extensive and included numerous car dealerships, banks, credit card companies, furniture stores, department stores and communication service providers. Trans Union did place Fraud Alerts on our credit reports at this time. I also contacted Experian and Equifax and was dismayed to learn that they too showed numerous inquiries into our credit reports during the same 60 day period.

In speaking with the credit reporting agencies I also learned that aside from an excessive number of credit inquiries into our credit reports, our credit reports now also contained numerous address changes. These address changes were entered into our credit reports without any verification of their accuracy. We've resided at the same address in Ohio for twenty years, yet our credit reports now showed us living at six different addresses in Illinois.

It seems rather incomprehensible that our previously impeccable credit reports, which clearly showed wise and careful use of credit along with a stable twenty year residence history, now showed over twenty five unauthorized credit inquiries and six out-of-state address changes, all of which had been entered on our credit reports between September and November of 1999. Had the merchants or credit reporting agencies contacted us by phone or mail to notify us that a credit application had been submitted using our names and SSN's but the address on the application did not match our address of record, much of the criminal activity would have been "nipped in the bud". An address discrepancy between a credit application and the address of record on a credit report should not be ignored by the merchants or the credit reporting agencies, identity thieves often use a phony address and phone number. It is imperative that a system of "checks and balances" be implemented and adhered with by the merchants and the credit reporting agencies. Credit bureaus must verify the accuracy of the information received prior to posting information on credit reports. The credit reporting agencies can use available technology to "red- flag" information that does not fit the profile of the consumers' previous spending habits. Change of addresses need to be verified by the credit reporting agencies prior to changing the address on the consumers' credit report. The information sold and disseminated by the credit reporting agencies to the various lenders and merchants making credit inquiries is perceived by these banks and merchants as accurate because "it came from the credit bureau". It seems incongruous to have banks and merchants rely on the information appearing on credit reports when this information has been entered without any verification of its accuracy.

As our ID Theft saga continued, I filed additional police reports, and I followed the advice of the Trans Union fraud representative and attempted to make phone contact with all of the merchants who appeared on the inquiry page of our credit reports. These efforts were extensive, time consuming and extremely frustrating. I was placing phone calls to these merchants in an attempt to "put them on notice" that we had not applied for any credit. Many times these phone calls were only answered by automated phone prompt systems that never offered me the option of pressing an extension to speak to a human being. I was often asked by the phone prompt to enter an account number. I did not have the account number because I was not the one who opened the account. I did make efforts to try to circumvent the automated phone prompts. I pretended I was calling from a rotary phone, which led me into a voice response automated prompt system, and I pressed zero hoping a "live person" would come on the line. These efforts were frustrating, time consuming, and often futile.

I also placed numerous calls to various state and federal agencies as I attempted to weave my way through the maze of credit fraud and Identity Theft. The office of the Ohio Attorney General suggested that I contact the Federal Trade Commission (FTC). My call to the FTC led me to their ID Theft Clearinghouse (877 438 4338). Kathleen Lund was the Identity Theft counselor with whom I spoke. Kathleen confirmed, based on the facts that I gave her, that we were victims of Identity Theft. Kathleen informed me of Title 18 Section 1028 of the US Code which made Identity Theft a federal offense. Kathleen provided me with invaluable information, guidance and emotional support

during this extraordinarily stressful time. It was a pleasure to finally speak with someone who had a clear and thorough knowledge of credit fraud and Identity Theft. It was also a great relief to finally speak to a human being after the automated answering prompt hell I had endured as I attempted to contact the merchants. Kathleen started a file on our ID Theft case and gave me the assigned file reference number to include in our police reports. She advised me to contact the SSA and the BMV to report the fraudulent use of my husband's SSN. Kathleen advised me to keep a running log of all calls and contacts relative to our ID Theft nightmare, and asked me to keep her informed of any new developments. Kathleen's assistance, guidance and advice were very helpful. However, it is the Identity Theft victim who bears the burden of the Herculean task of trying to clear their good name and restore their good credit.

As I continued my efforts to contact the merchants, I received three very alarming phone calls. The date was now November 18, 1999, three days after we placed the Fraud Alerts on our credit reports. The first call was from Citibank in Illinois alerting us that a twenty five thousand dollar ($25,000.00) personal loan application had just been made by someone using my husband's name and social security number. The loan application had been made in person by an impostor posing as my husband. This impostor had presented legitimate looking identification. Our credit reports were pulled as the loan officer was processing the loan application, and we were contacted because of the Fraud Alerts on our credit reports. I spoke to the fraud department of Citibank and explained that we had placed the Fraud Alerts on our credit reports three days prior when we became aware we were victims of Identity Theft. Citibank's fraud department said they would contact their security department, check to see if the impostor was on their surveillance tape, and call me back.

As I was waiting for the return phone call from Citibank, I received another alarming phone call. Thomas Retkowski, a fraud investigator from Bank One's regional fraud office in Wisconsin, called to inform us that a fifteen thousand dollar ($15,000.00) personal loan application had just been made in Illinois by someone using my husband's name and SSN... The Fraud Alerts on our credit reports prompted Thomas to call. I informed Thomas of the call I had received from Citibank just minutes before his call, and told him we were victims of Identity Theft. Thomas faxed us an affidavit to sign and have witnessed. I told Thomas we had filed police reports and had been in contact with the FTC. Thomas wanted us to immediately fax the signed affidavit back to him in Wisconsin. As the faxes were being sent, another call came in. Marquette Bank in Illinois had just received a five thousand ($5,000.000) loan application from someone using my husband's name and SSN. I told the fraud investigator from Marquette Bank about the two other fraudulent loan applications and the affidavit we were in the process of faxing to Thomas Retkowski.

Three different banks, all within close geographic proximity to each other in the greater Chicago area, had just received three fraudulent personal loan applications for varying amounts of money by an impostor using my husband's name and SSN. These fraudulent loan applications were all made in less than a two hour time period and they totaled forty-five thousand dollars ($45,000.00). The impostor had come into each bank,

sat down with a loan officer, filled out the necessary paperwork, presented legitimate looking photo identification as “Raymond Mitchell”, and told each loan officer that he would come back to the bank to pick up “his” money in about an hour.

Thomas Retkowski received our signed fraud affidavit at his office in Wisconsin as I was contacting our Ohio police department to report that an impostor was currently applying for loans in my husband’s name in Illinois. Aside from the emotional and psychological trauma we were enduring as victims of ID Theft, we now found ourselves embroiled in a very tension filled, time constraint driven drama that was unfolding before our eyes. We were dealing with three different banks in Illinois, communicating with a fraud investigator in Wisconsin, and filing an Ohio police report. To complicate matters further, we were dealing with two different time zones and we had a one hour window of opportunity before the impostor returned to the bank to pick up “his” money.

Thomas Retkowski’s fraud investigation expertise and initiative synchronized well with the outstanding police cooperation we received from Chief Edward Matty and Sgt. Robert Verdi of our local Ohio police department. As a result of their coordinated efforts, plainclothes detectives from Lansing Illinois were in place at Bank One within the hour, awaiting the arrival of the impostor. The impostor returned to Bank One to pick up “his” money and was arrested as he exited Bank One after having fraudulently obtained the fifteen thousand dollars ($15,000.00). The impostor had five thousand dollars ($5,000.00) in cash and two five thousand dollar bank checks ($10,000.00) made payable to Raymond Mitchell. The money was recovered when the impostor was arrested. I was told by the arresting detectives that the impostor also had an Illinois driver's license and an Illinois State Identification Card, which displayed the impostor’s picture along with my husband's name and SSN.

The detectives ran the fingerprints of the impostor, and discovered the impostor had 17 aliases and a twenty three year criminal history. A preliminary hearing was set for November 20, 1999, and the detective said he would keep me informed of any developments.

I continued to make phone calls to try to resolve this nightmare when I learned that the impostor was released on a signature bond in his own recognizance at the preliminary hearing. Words can't even begin to describe the horror I felt knowing that a suspect with seventeen aliases, multiple priors and an extensive criminal background was released on a signature bond in his own recognizance. The hearing was in Cook County, Illinois and the Judge was Thomas Panicki. I was also told that when this suspect was arrested he had stated to the detectives: "I didn't use a gun, I didn't use a knife, call my lawyer I will plead guilty and they will put me on probation".

It was appalling for me to realize the criminals commit these crimes with a premeditated methodology that accomplishes their criminal intent with the least possible risk for the criminal, if apprehended, serving jail time. These criminals are still committing bank robbery, fraud, identity theft, forgery and a litany of other criminal acts, however, since a traditional weapon was not used, the criminals, if apprehended, are

counting on probation instead of incarceration. The criminal misuse of technology that allows these impostors to fraudulently manufacture the documents necessary to steal the identity of another should be classified as a weapon, as serious a weapon as a gun or a knife. The criminal misuse of technology has become the Identity Theft impostor's weapon of choice.

The scales of justice are tipped in the wrong direction when an identity theft criminal is sentenced to serve a shorter period of incarceration than the length of time it takes the Identity Theft victim to clear their credit report and restore their good financial reputation! The jail sentences imposed on ID Theft criminals by state and federal courts need to be of sufficient duration to serve not only as a deterrent, but to truly reflect the egregiousness of these crimes.

As our Identity Theft saga continued, some of the cooperative merchants honored our requests and sent us copies of the fraudulent applications. These fraudulent applications contained numerous blatant errors that should have alerted the merchants and the banks that something was amiss. One example is an application that was made to purchase a Ford Expedition. This vehicle was purchased using my husband's name and SSN along with the name and SSN of a co-buyer. These two men presented themselves to the car dealership and said they resided together. However, on the application one man filled out his address as 2243 N.Grand and the other used 2243 W.Grand. On this same application, the phone number that was listed to verify place of employment had an area code of 300, this area code is not a valid area code in the continental United States. The criminals also purchased the 5 year 60,000 mile extended warranty which appeared on the application at a cost of $695.00. Yet, when this figure was carried over to the debit column to determine the amount of credit to be granted, the figure became $1695.00 instead of $695.00. The Raymond Mitchell impostor did not present a driver's license for identification; he used a janitorial services photo identification card. However, the signature on the janitorial services ID card did not match the criminal's signature on the loan application. And to top off the list of blatantly obvious errors on this application, our last name was misspelled! Our last name was not only misspelled on the loan application, it was also misspelled on the fax from the lender approving the loan. In spite of these GLARING "red flag" discrepancies, this loan was approved and these two men purchased a Ford Expedition using our credit history. Had this transaction been processed using due diligence and an iota of common sense these blatant discrepancies would have been caught. The possibility does exist that these criminals made the purchase through a car salesman, car dealership and lender that were co-conspirators, but I think that is a remote possibility. I do firmly believe that sloppy business practices substantially contribute to the criminal's ability to successfully defraud merchants and lenders. Shoddy business practices are abetting criminals in committing the crimes of credit fraud and Identity Theft, and plunging innocent victims into ID Theft hell. It was due diligence that was exercised by a salesperson in an Illinois furniture store that prevented the extension of credit when an impostor tried to purchase furniture. The salesperson realized that "something wasn't right" after reviewing the credit application. Credit was not extended by the furniture store and the criminal was thwarted in this

fraudulent attempt. I think this is a good example of how good business practices can diminish fraud.

In spite of the extensive time and effort we logged in trying to resolve this Identity Theft nightmare, we now had “derogatory accounts” appearing on our credit reports. We were also receiving phone calls from collection specialists. The Ford Expedition was not the only vehicle purchased by criminals using our credit history. We learned that a Lincoln Navigator had also been purchased by impostors when we received a phone call from a collection specialist who wanted to know why we were overdue on the payments for “our” Lincoln Navigator. I tried to nicely explain to these collection specialists that we were victims of Identity Theft and we did not purchase these vehicles or open the accounts they were calling about. I provided them with the name and phone number of the detectives, the police report number(s) and the reference number assigned by the FTC. I strongly suggested they not call me back unless they were willing to provide whatever information and documentation they might have to assist in the investigation. I always ended my conversation with the collection specialist by saying: "It's amazing to me that you can find the real Ray and Maureen Mitchell when you want to collect your money, too bad you didn't find the real Ray and Maureen. Mitchell before you loaned out the money."

We were able to determine from pictures we received from the car merchants that the criminals who purchased the vehicles were not the same person, and they were not the impostor who was apprehended leaving Bank One. We had been victimized by a sophisticated Identity Theft ring that operated in an organized and insidious manner.

The detectives told us that the criminals know when the fraud alerts on our credit reports will expire. The fraud alert was in place for two years, and if we failed to reactivate the fraud alerts our information would be re-circulated through the criminal ring again. Therefore, we will have to keep fraud alerts on our credit reports for the rest of our lives. So, in the future, when my husband and I apply for credit we will have to explain this nightmare to the lender, hope they believe us and hope they don't perceive us to be the criminals.

Our efforts to restore our good names and good credit history were extensive. I made hundreds of phone calls and I sent dozens of notarized, certified, return receipt requested letters to the merchants informing them that the applications they received were fraudulent. We submitted numerous affidavits, notarized statements and notarized handwriting samples. We filled out over twenty different sets of forms and documents in our attempt to comply with the merchant’s requests for further information. The paperwork nightmare that we endured during our initial victimization was horrendous, and it added insult to injury. Seemed rather ironic that a criminal could fill out a fraudulent application, obtain credit in our names and easily have our address changed, yet, when we tried to dispute fraudulent accounts and have our address “corrected” back to our real address, we were inundated with paperwork requiring us to “prove” our identity and address.

A distressing and frustrating incongruity exists for victims of Identity Theft: the criminal is assumed innocent until proven guilty, but the Identity Theft victim is assumed guilty until proven innocent. The criminal can have a public defender appointed to protect his legal rights, however, if the Identity Theft victim needs to hire an attorney to assist in clearing their names and restoring their credit they will be paying substantial legal fees out of pocket.

We had exhausted all known resources in an effort to clear our names and restore our credit. I met with our Ohio Congressman, Steven LaTourette. It was through Congressman LaTourette's intervention and assistance that I was able to meet with the FBI. I met with numerous police officers. I met with a Victim's Assistance Program in Ohio and I contacted a Victim Advocacy Program in Illinois. I spoke to prosecuting attorneys, and sent packages of information to State's Attorneys. I begged, pleaded and cajoled to try and obtain a federal investigator and a United States' Attorney to take our case. The Lansing Illinois detectives who apprehended the Bank One impostor were limited to investigating crimes occurring within their jurisdiction. Identity Theft crimes are frequently cross-jurisdictional. Cooperation and coordination among federal, state, and local law enforcement agencies is of paramount importance to the successful investigation and prosecution of ID Theft cases.

I had frequent contact with Kathleen Lund, our ID Theft counselor at the FTC, as I attempted to continue to navigate my way through the labyrinth of Identity Theft hell. The input and support I received from her continued to be valuable and helpful. Kathleen asked for and obtained my consent to submit my name to be contacted by a member of the office staff of Senator Jon Kyl (R-AZ). Senator Kyl was going to chair an Identity Theft hearing, and wanted to have an Identity Theft victim testify at this hearing. I received a call from Jim McDermond, one of Senator Kyl's staff members. Jim requested information and documentation from me, which I gladly sent him. I was invited to testify at the hearing, which was held March 7, 2000. It was the Hearing before the Senate Committee on the Judiciary Subcommittee on Technology, Terrorism, and Government Information: "ID Theft: When Bad Things Happen to Your Good Name". It was my privilege to testify.

In my opinion, many good things were accomplished as a direct result of that hearing. Chairman Jon Kyl exhibited a sincere interest and determined intent to diminish the prevalence of ID Theft crimes. Chairman Kyl also showed great empathy for the trials and tribulations a victim of ID Theft endures and a sincere desire to make the system more "victim" friendly. On the last page of my Senate testimony, I included a list of 15 recommendations that I felt were important from my perspective as an ID Theft victim. One of my recommendations to the Subcommittee was to implement a uniform ID Theft victim reporting affidavit. As stated earlier, as victims of ID Theft we had been required to fill out dozens of different affidavits and follow dozens of different protocols to satisfy the merchants' requests for information and documentation as we tried to dispute fraudulent charges and restore our credit. I am pleased to say that through the intervention of Senator Kyl, the Subcommittee, and the FTC there is now a uniform ID Theft Affidavit. This ID Theft Affidavit will substantially diminish the amount of time

an ID Theft victim has to spend filling out forms and paperwork as they try to restore their credit and dispute fraudulent accounts.

My extensive efforts to try to obtain a federal investigation into our ID Theft case were unsuccessful. Senator Jon Kyl and James McDermond intervened, and that resulted in the United States Secret Service and Postal Inspection Service initiating a federal investigation. Richard Starmann, USSS; Christine Hoskins, USPIS; and Robert Himmelein, SSA/OIG all became involved in investigating our case.

Shortly after the federal authorities became involved in our case, I learned the fate of the Ford Expedition, the same Ford Expedition that had all of the glaringly obvious errors on the loan application. The criminals who had fraudulently purchased the Ford Expedition had torched the Ford Expedition and filed a fraudulent insurance claim in my husband's name. The criminals were now seeking to collect the insurance proceeds from this arson. As a result of this, we were now also dealing with the National Insurance Fraud Bureau. We were required to notify our own insurance company to put them on notice that the fraudulent insurance claim was filed by criminals, not by us. These criminals had collectively applied for $150,000.00 worth of new loans in our names, trashed our credit, filed a fraudulent insurance claim, and committed arson in my husband's name.

As victims of Identity Theft, our lives were turned upside down. We lived with a degree of fear that permeated every aspect of our lives. We not only placed the Fraud Alerts on our credit reports; we placed security protocols on our bank accounts that required photo ID and password (not mother's maiden name) for any transaction; canceled our credit cards; alerted our employers; notified the IRS; placed 7 year consumer statements on our credit reports and alerted our medical insurance company. Identity Theft had violated many areas of our lives.

Through the cooperation of our local police department, Chief Edward Matty wrote a letter on police letterhead stationary that stated we were the victims of financial crimes and Identity Theft. This was a notarized letter signed by Chief Matty. Identity Theft criminals were committing crimes using our names, and potentially having arrest warrants issued under our SSN's. I carry this letter with me at all times, as does my husband and both of our adult children. We all run the risk of being subject to mistaken arrest if we are pulled over for a traffic violation and arrest warrants appear under our SSN's numbers.

At the time I testified to the Senate Subcommittee, I had logged over 400 hours of time trying to clear our names and restore our good credit. I had accumulated hundreds of pages of ID Theft paperwork and documentation. Words are unable to adequately express the gamut of emotions that we have experienced as victims of ID Theft. The impact of being a victim of Identity Theft is all encompassing. It affects you physically, emotionally, psychologically, spiritually and financially. This has truly been a life altering experience.

Identity Theft has become a national epidemic. Banks and merchants are being defrauded out of billions of dollars each year by Identity Theft criminals. Innocent victims are having their credit ruined and financial reputations destroyed. We all pay the price through the higher cost of consumer goods, and higher interest rates on loans and credit cards. This epidemic must be stopped. The compromising of real identities is now the weakest link in the chain of financial transactions.

Once you become a victim of Identity Theft your life is forever changed. We still feel like we are "waiting for the other shoe to drop". We did not know how many more accounts might still be outstanding, we did not know if a collection specialist was calling when our phone rang and we did not know if our good names and financial reputations would ever be truly restored.

What we did know was that the impostor who had been arrested on November 18, 1999 by the Lansing Illinois detectives, the one who had been released on the signature bond in spite of an extensive criminal background and 17 aliases, appeared in court as the case progressed. This criminal was interviewed numerous times by the federal investigators and offered sentencing consideration in exchange for divulging accurate information. He declined to disclose any information, and was eventually sentenced to three years in the Illinois Department of Corrections. The time he actually served amounted to a little more than a year.

Our lives would never return to the “normal” status we had enjoyed prior to becoming ID Theft victims. The criminals receive a sentence of a specific duration, the ID Theft victim’s sentence lasts for the rest of their life. There are frequent and often daily reminders of the trauma we endured as ID Theft victims. However, we thought the worst of the ID Theft nightmare was now behind us. That turned out to be wishful thinking on our part.

In the spring of 2001 we were in the process of trying to purchase a second home at the western end of Ohio, about 150 miles away from our primary residence. Both of our adult children are students in that vicinity, and purchasing a home there would substantially reduce the rent and dormitory expenses they were incurring. Our credit reports had been cleared of all of the derogatory accounts that had appeared as a result of our ID Theft victimization, and we proceeded with the intended purchase. As I stated earlier, I am a licensed Realtor, therefore, I am very familiar with the mortgage loan process. We wrote an offer to purchase a home, and I went to the KeyBank branch in that area to transfer the earnest money deposit from our savings account to our checking account. Please note that I had placed security protocols on all of our accounts as a result of our ID Theft victimization in 1999. Our local KeyBank branch employees had been honoring the protocols since I placed them on the accounts. Yet, when I transferred the money at an out of town KeyBank branch where I had never before done any transactions, I was not asked to present my photo ID or give my password. I informed the branch manager of the required protocols, and she reviewed our account information, which was displayed on the teller’s screen. The manager scrolled through quite a few computer screens before the security protocol information appeared that stated our

accounts required photo ID and password. I found this to be not only absurd, but totally unacceptable. I insisted that the security protocols appear on each and every screen of our bank accounts, and the branch manager phoned our home branch of KeyBank to ensure that this was accomplished. The account screens were reviewed to verify that the tellers were prompted on every screen to require the security protocol.

After our offer to purchase was accepted, I started the mortgage application process. I chose a lender that I had done business with in our home community that had a branch office in the area in which we were purchasing the second home. I had forewarned the loan officer to expect to see Fraud Alerts and consumer statements on our credit reports and I told her we had been victims of ID Theft. I made the mortgage loan application in person, presented my driver's license, showed the loan officer my letter from Chief Matty and a copy of my Senate Subcommittee testimony. All appeared to be going well, until the loan officer pulled the copies of our credit reports. There was now a "derogatory account" appearing on my husband's credit report. Remember the fraudulent purchase of the Ford Expedition by the Illinois criminals in 1999? The one where there were multiple glaringly obvious errors on the fraudulent credit application. The same one that was torched and criminals filed the fraudulent insurance claim in my husband's name. The bank that financed the Ford Expedition, Firstar Bank, had posted a "derogatory account" on my husband's Experian credit report. This "derogatory account", which had never previously appeared on our credit reports, lowered my husband's FICO credit score by 118 points and we ran the risk and embarrassment of being denied the mortgage loan for the home we were legitimately trying to purchase. I was livid!

I now had to again battle with the credit reporting agency to have this "derogatory account" removed from this credit report. My previous and rather extensive efforts in having fraudulent accounts removed from our credit reports had been a very time consuming process. However, time was now of the essence in getting this "derogatory account" removed from the credit report. Our purchase agreement for buying the home contractually required that we obtain loan approval within 25 days or we would lose the house. I was frantic as I started making the calls to try to have this remedied.

I again contacted Kathleen Lund at the FTC to let her know about the "derogatory account". I also contacted Sen. Kyl's office, and Jim McDermond assisted us in trying to get the "derogatory account" removed. Experian did eventually remove the "derogatory account", but it required great effort on my part and Jim McDermond's part to get this accomplished. The real Ray and Maureen Mitchell were almost unable to legitimately obtain a mortgage loan, in spite of the extensive efforts I had expended cleaning up our credit. My friend, Cathy Teschke, summed it all up when she stated to me: "You know, Maureen, you should have had the criminals apply for the mortgage loan; they would have gotten it with no problem!" There may be more truth than any of us care to admit in Cathy's statement.

The mortgage loan was finally approved, and we again hoped our ID Theft nightmare was behind us. We learned that it wasn't as we attempted to purchase and

finance a refrigerator for the house we just bought. Best Buy had a 12 month same as cash promotional offer on appliances, and we applied for this promotional financing. We were denied the credit for the purchase of the refrigerator. As embarrassing as it was to be denied credit to purchase the refrigerator, it was gut wrenching to realize that our credit worthiness might never truly be restored. Criminals had no trouble obtaining credit in our names, but now we couldn't even finance a refrigerator!

Our next ID theft problem surfaced on October 30, 2001. I received a phone call at home from a woman who identified herself and said she was a KeyBank branch manager. She was calling to ask if we were having "trouble" with our bank accounts. I told her we were victims of ID Theft and had security protocols on our KeyBank accounts. She said she was placing a "security freeze" on our accounts, and I would be contacted by a KeyBank fraud investigator. I obtained the information I needed to reach her and to verify that she was a Keybank employee. I then contacted our local KeyBank branch, spoke to an employee I had known for years, gave her my password and asked her to check our accounts. There was indeed "trouble" with our bank accounts, and a security freeze had just been placed on our accounts. Four fraudulent withdrawals had been made from two of our Keybank savings accounts, and it was the attempt at a fifth fraudulent withdrawal that finally prompted KeyBank to contact me. The withdrawals were not made at our local KeyBank branch; they were made at three different Keybank branches in the greater Cleveland area. Criminals successfully made four fraudulent withdrawals, from two different savings accounts at three different KeyBank branches in spite of our security protocols requiring photo ID and password. I was stunned and furious! How the hell this could have happened was beyond my ability to comprehend. These fraudulent withdrawals collectively totaled $34,006.50. Criminals absconded thirty- four thousand six dollars and fifty cents from our bank accounts! And, as a result of the security freeze that was placed on our accounts, we had no access to our own money! We had banked with KeyBank for close to twenty years and were well known to the employees at our local branch, yet we had no access to our own money. Words will never adequately express the emotional turmoil we were experiencing as a result of our security protocol protected savings accounts being infiltrated by criminals.

The dates of the fraudulent withdrawals from our KeyBank accounts were two years after our initial ID Theft victimization. We knew the fraud alerts on our credit reports were good for two years, and I had conscientiously and intentionally renewed the fraud alerts well before the fraud alerts were set to expire. My intent in renewing the fraud alerts early was to try to stay one step ahead of the criminals. However, instead of criminals fraudulently applying for out-of-state loans in our names, they were now infiltrating our security protocol protected bank accounts in our home state, in essence in our own back yard. The criminals in Illinois who fraudulently obtained credit were impostors posing as my husband. Now there was a criminal impostor posing as me in Ohio. The resulting fear that now permeated the very essence of our being is indescribable.

I was again filing yet another police report, and also filing a KeyBank "Affidavit of Fact" report. Contact had been established with the KeyBank fraud investigator, Fred,

and an investigation into the events was initiated. Fred confirmed our accounts were frozen and told us that no activity would occur on the accounts. I had dozens of questions that I wanted answered immediately. One of the first things I wanted to know was how the hell criminals were able to withdraw the money with the security protocols in place. And I asked if the security protocols were even followed. Fred stated that the bank was "looking into it". I also wanted to know if the criminals had used our password. We needed to know immediately as to whether or not our password was compromised. Fred was unable to give us an answer. I also inquired if the same KeyBank teller was involved in each of the four fraudulent withdrawals. Fred said he would find out and let me know. I asked lots of questions, unfortunately, I did not receive many answers. My conversation with Fred, in my opinion, was not going very well. He was unable to answer my questions, and I wanted immediate answers. I also perceived a degree suspicion emanating from Fred that was directed at us. Fred seemed to be questioning our integrity, which I greatly resented. We are not criminals, we had not made nor had we authorized the withdrawals; we were previous ID Theft victims who had insisted on placing the security protocols on the accounts in the first place. The conversation went from bad to worse when Fred stated that after KeyBank investigated the circumstances of the fraudulent withdrawals "the money would probably be restored" to our accounts. I was irate to hear "probably restored". I stated to Fred, in no uncertain terms, that since KeyBank had allowed criminals to infiltrate our security protocol protected bank accounts not once, not twice, but four different times "there is no probably about it, our money will be restored, with interest!" I strongly suggested to Fred that he secure the bank surveillance tapes and pull our signature cards to prove to him that we were not the ones who made the withdrawals.

I asked Fred the date of the first fraudulent withdrawal; he told me it was done on Oct. 26, 2001. I then asked Fred for the date that KeyBank cut their Oct. statement; he said Oct. 25, 2001. I pointed out to Fred that the first fraudulent withdrawal was made the day after KeyBank cut their monthly statement. These dates were significant in my mind because the KeyBank statement that was due to arrive in my mailbox at any minute would not show the fraudulent withdrawal because it had been made right after the monthly statement was issued. Therefore, the criminals would have had a one month "head start" before the withdrawal would appear on my bank statement. I asked Fred if that did not indicate to him a "degree of sophistication" on the part of the criminals. Fred replied to me that it was "coincidence". I do not think it was "coincidence"; I think the criminals are smarter than many of the investigators.

We learned that three of the fraudulent withdrawals were in the amount of six thousand ($6,000.00) each, and the fourth fraudulent withdrawal was in the amount of sixteen thousand dollars ($16,000.00) The $6.50 appeared as a "charge" to our account posted on the same day that three out of the four fraudulent withdrawals had been made. And, in spite of the fact that there was thirty-four thousand six dollars and fifty cents ($34, 006.50) missing from our now frozen bank accounts, Fred was focusing on the six dollars and fifty cents ($6.50). Fred stated that the "six dollars and fifty cents" withdrawal from our accounts "must have been done" by us. I again firmly and emphatically told Fred we had not made any of the withdrawals. Fred then told me he

found it hard to believe that "a criminal would withdraw $6.50". I told Fred that I was not a fraud investigator; however, by now I felt that I had earned a PhD. from the school of ID Theft hard knocks and that I could think of two reasons for the $6.50 withdrawal. One reason was that criminals might have been testing the accessibility of the accounts between major withdrawals, and the other more likely reason was that the criminal took all or part of a withdrawal in the form of a bank check and the $6.50 was the chargeback to the account for the cost of the bank check. Turns out, I was right about the charge-back. When the criminal made the $16,000.00 withdrawal, she took half in cash and half in the form of a bank check. And, the bank check had been issued payable to Maureen Mitchell!

The fact that this bank check was made payable to Maureen Mitchell is very significant. This impostor now had in her possession an $8, 000.00 bank check issued in my name. Each time an impostor obtains an official piece of documentation in the name of the victim it gives the impostor additional "credibility" in assuming the identity of the victim. KeyBank not only gave our money to an impostor on four different occasions, KeyBank also gave the impostor a bank check in my name.

Additional problems arose for us as a result of our frozen bank accounts. All of our KeyBank accounts were frozen, not just the accounts the criminals had infiltrated. The criminals had not infiltrated our checking account, but we were now unable to write checks or access any of our KeyBank funds. We had bills that were due to be paid: mortgage payments, utility bills, credit card bills and college tuition to name a few. We asked how long the freeze would remain on our accounts, but no one from KeyBank could tell us when the accounts would be unfrozen. To complicate matters further, there were four checks that we had written just days before our accounts were frozen that had not cleared our checking account before the freeze was placed on our accounts.
I asked Fred what would happen to those checks; Fred told me the checks would be returned. I asked Fred if that meant the checks would come back "insufficient funds", Fred said the checks would be returned stamped "refer to maker". I requested that these four checks be allowed to clear our checking account, and offered to provide KeyBank with each check number, the amount the check had been written for, and the name of the entity to whom the check had been made payable. These checks had been written by us to our grocery store, our newspaper carrier, our church and my alumni association. Fred said he could not allow these checks to clear our account even though I could provide all of the information contained on these checks. As a result of the return of these checks to the payee stamped "refer to maker", we received a letter in the mail from a collection agency. This letter stated that we had been turned over to collections for the check that we had written to our grocery store, as it had not been honored by KeyBank. The letter stated that there was a $30.00 collection charge that was added to the amount the check had originally been written for, and went on to say this collection agency "has been designated to collect payment and will record your checking account number in our check verification database, which can affect your check cashing ability at many retail establishments." As a result of KeyBank's failure to honor this check we were placed on a "bad check list".

I showed our local KeyBank branch manage the letter from the collection agency, and efforts were made to get our names and checking account number out of the collection agency's database and to waive the $30.00 collection penalty. Those efforts were unsuccessful until I contacted the owner of the grocery store, explained the events that lead up to the frozen accounts, which resulted in the check not being honored and returned "refer to maker". The grocery store owner then contacted the collection agency and the situation was eventually resolved.

My contacts with Fred continued, and I received additional information from contacts I initiated with the KeyBank branches where the fraudulent withdrawals had been made. I asked for a physical description of my impostor. I was told she was "a 5'5" brown eyed African American with auburn hair pulled back in a French twist" and that she was "calm and svelte". I am a 5'3" Caucasian American with green eyes who by this time was far from calm and certainly not svelte. KeyBank's investigation continued, and our accounts remained frozen. I was still unable to access any of the money in our KeyBank accounts to pay our bills. And we were living with each day with a great deal of fear and uncertainty. The criminals had invaded the most private area of our lives, our personal finances and this second round of Identity Theft crimes had been committed in our home state. I was born, raised and educated in New York City and I am usually not a woman who gives in to fear, however, the trauma of being a two-time ID Theft victim was exacting a huge toll. Our entire family was affected by the stress. It's a horrible feeling to know that criminals are privy to your most private information. Some of our friends equated the trauma we were enduring as "financial rape". That's as close as any of us could come in trying to put into words what we were feeling. We were doing our best to cope with the fear and the rage. I was absolutely incensed that the security protocols on our KeyBank accounts failed to work, that our accounts were frozen, that we couldn't pay our bills and that we were placed on a bad check list with a collection agency.

On Sunday, Nov. 4, 2001, we received a phone call at home that added to our trauma. The caller identified herself as Joanne, and said she was calling from First North American National Bank in Georgia. Joanne wanted to know if I had just applied for a $5,000.00 line of credit at Circuit City. I quickly told Joanne that we were ID Theft victims, and had not applied for any credit. Joanne said she was calling because she saw the Fraud Alert on my credit report as she was trying to process a credit application that had just been made in my name. I asked Joanne to tell me the location of the Circuit City store where the application had been made. Joanne said she only had a location number for the store, not an actual store address. I told Joanne that I needed the address immediately, as we had just experienced local criminals infiltrating our bank accounts. Joanne promised to locate the store address and call me back. It was only a matter of minutes before Joanne called back, and told me the Circuit City store was located in North Randall Ohio. North Randall lies on the outskirts of Cleveland. Joanne put me on a conference call to the Circuit City store, and we spoke to the store manager. I told the store manager that if "Maureen Mitchell" was in the store applying for credit to pretend that the bank was working out a credit glitch, and it would take a few minutes before they could extend credit to her. I then told him that she was an impostor, I was the real

Maureen Mitchell and I wanted him to call the police immediately. He placed us on hold, walked to another phone and whispered to us that the impostor had been standing right next to him as we were speaking. He told us that he police were called, and that the impostor was still in the store. Within a matter of minutes the North Randall police arrived and arrested the impostor. I could hardly find the words to thank Joanne and the store manager. It was such a relief to know that an arrest had been made. One of the arresting officers picked up the conference call and told me they were transporting the suspect to the North Randall police station, gave me the station's phone number and instructed me to call there in 20 minutes. While waiting to place that call, I had the opportunity to continue to speak to Joanne. Joanne told me that she knew from the Fraud Alert and consumer statement on my credit report that I had been a victim of ID Theft. Joanne said she had spoken to the impostor on the phone as the impostor belligerently tried to assert that she was the real Maureen Mitchell. Joanne knew it was an impostor when she asked the impostor questions related to my credit report that only I would know the answer to. Joanne also told me that when the impostor filled out the credit application she had tried to change my address. The impostor even had the nerve to request that Joanne send her a copy of "her" credit report at the "her" address.

I called the North Randall police department and was told that the suspect they arrested possessed what appeared to be an Ohio BMV issued photo identification card. This card was issued in my name, had my home address, and my driver's license number. This card also had the impostor's picture! I asked the officer if it was a real BMV identification card, or had it been manufactured in some criminal's basement. I was told the card appeared to be an authentic BMV issue. I asked for a physical description of this suspect, and it was very similar to the description I had been given of the impostor who infiltrated our KeyBank accounts. I also asked the officer how the BMV could have issued a photo identification card that displayed my name, my address, and my driver's license number to a woman who looked nothing like me. My photo had been in the Ohio BMV's data base since I got my Ohio driver's license in 1978. The officer told me I would have to ask the BMV those questions. I told the officer of our ID Theft victimization, and that an impostor had recently made fraudulent withdrawals from our KeyBank accounts. I was speaking with this officer on a Sunday night and was told I could call the station on Monday morning and the officers would have more information.

On Monday morning I placed numerous phone calls to the Ohio BMV to find out how an impostor could have obtained an identification card from the BMV that displayed my personal information but the impostor's picture. I eventually reached an investigative officer of the BMV and was appalled to learn that not only had the BMV issued the photo identification card to the impostor, the BMV also suspended my driver's license when the impostor obtained the photo identification card. I couldn't believe what I was hearing; my driver's license had been suspended! I asked the investigator how that was possible and he explained that in Ohio it is illegal to concurrently have an Ohio driver's license and an Ohio BMV issued photo identification card. When the impostor obtained the photo identification card, she signed away my driving privileges in the state of Ohio for life, and my license was suspended. I then asked why I wasn't notified by the BMV that my license was suspended, and I was told they would eventually send me a letter. I

inquired as to the date my license suspension occurred, and was told it was Oct. 25, 2001. That was the day before the impostor made the first fraudulent withdrawal from our KeyBank accounts. I was also told that I would have to meet with a BMV fraud investigator at a Deputy Registrar's office of my choosing. I asked if they would like me to "flap my wings to get there"; they had suspended my driver's license. I was also instructed to bring plenty of proof of identification because I would have to prove I was the real Maureen Mitchell. I asked if they would like to use my suspended driver's license as valid proof! I was also told that as a "courtesy" the State of Ohio would waive the requirements for the written test, the road test and the re-licensing fee.

I was absolutely heartsick to realize our bank accounts were frozen, our names were on a bad check list and my driver's license was suspended. I hold three licenses in the State of Ohio; my driver's license; my real estate license; and my R.N. license. After learning my driver's license was suspended, I was extremely fearful that my professional licenses might also be suspended as a result of the actions of my impostor.

I met with the BMV fraud investigator and brought my entire briefcase full of Identity Theft paperwork. I showed him the notarized letter from Chief Matty and gave him a copy of my Senate Subcommitee testimony. He then went through the BMV required protocol to issue me a new driver's license. He faxed the necessary forms to Columbus to obtain a Columbus issued driver's license number that was supposed to be "coded" to let law enforcement know that it was a re-issued license to an ID Theft victim. I sat for the driver's license picture, and waited for the license to be processed. I was astounded when I read the physical description that was printed on my new license. My new license said I was 5'5" with brown eyes! The criminal's information overrode my information in the BMV database. We had to start the whole process over again, and the Deputy Registrar had to manually type in my correct physical description.

When KeyBank was finally ready to unfreeze our accounts, we arranged to close our accounts. We still do not know if the KeyBank tellers who gave my impostor our money were complicit or inept. The facts, as we saw them, were that KeyBank could not keep our money safe; therefore, KeyBank would no longer have our money. KeyBank unfroze our accounts during non-business hours and cut us cashier's check to close the accounts.

I contacted Kathleen Lund at the FTC to update her on the arrest of my impostor. I also informed Fred, the KeyBank fraud investigator, of the arrest. We were eventually told that the impostor who had been apprehended at the Circuit City store confessed to the fraudulent KeyBank withdrawals. My impostor also had a criminal history, and is currently incarcerated on probation violations. She was indicted by the Cuyahoga County grand jury on Identity Theft charges. I registered with the Cuyahoga County Witness/Victim Service Center, and will be kept informed of the judicial process as it progresses. Our case is currently pending

As victims of Identity Theft we will always carry the emotional, psychological, and financial scars. To this day we still do not know how the criminals obtained our personal information. Our "point of compromise" has yet to be determined.

We hope and pray that our Identity Theft nightmare is finally over.

The tragic and horrific events of September 11, 2001 serve as a horrible reminder of the extent and the reach of the crime of Identity Theft. Congressional testimony delivered in November 2001 revealed that the 19 hijackers had multiple aliases and several assumed identities. Some of the hijackers had more than one SSN. James Huse, the Inspector General of the SSA testified: "We know now, without question, that this illegal activity not only facilitates financial crimes but provides capability for organized criminals to sustain themselves while engaged in acts of terrorism." Identity Theft is not only wreaking havoc with the lives of its victims, Identity Theft is funding terrorism.

The epidemic of Identity Theft must be stopped. ID Theft crimes have cost our country billions of dollars in recent years. On September 11, 2001 Identity Theft facilitated terrorism and cost our country thousands of lives.

Thank you for the opportunity to submit this testimony.

Respectfully submitted,

Maureen V. Mitchell